Защитите себя и своих близких от киберпреступников.

В условиях активного использования мобильных устройств, социальных сетей, а также внедрения бесконтактных способов оплаты, существенно возрастает риск неправомерного получения персональных данных граждан злоумышленниками.

Методы, применяемые мошенниками для завладения личной информацией, становятся все более изощренными. Одним из распространенных приемов является телефонный звонок якобы от родственника или сотрудника правоохранительных органов. Гражданину сообщают о чрезвычайной ситуации, например, участии близкого человека в дорожно-транспортном происшествии – и предлагают урегулировать вопрос «в досудебном порядке», переведя определенную сумму на указанный номер телефона. В подобных ситуациях следует сохранять спокойствие и в первую очередь самостоятельно связаться с упомянутым родственником. В большинстве случаев информация, переданная по телефону, оказывается ложной.

Распространены случаи получения SMS-сообщений с информацией о якобы заблокированной банковской карте или зачислении денежных средств от неизвестного отправителя. В ответ граждан предлагается перезвонить или выполнить иные действия, направленные на передачу конфиденциальных данных. Настоятельно рекомендуется не совершать звонки на неизвестные номера, не следовать указаниям лиц, представляющихся сотрудниками банков, и ни в коем случае не передавать им сведения о своей карте, включая пин-коды и одноразовые пароли. При возникновении сомнений необходимо лично обратиться в банк или позвонить на официальную горячую линию.

Отдельного внимания заслуживают случаи мошенничества, направленные на граждан пожилого возраста. Злоумышленники предлагают приобрести дорогостоящие лекарства, биологически активные добавки либо медицинское оборудование, обещающее «чудодейственное» исцеление. При посещении квартиры посторонними лицами, представляющимися сотрудниками организаций, рекомендуется уточнить цель визита, запросить документы и при возможности связаться с управляющей компанией для проверки информации. До выяснения обстоятельств впускать неизвестных в квартиру не следует.

Кроме того, участились случаи рассылки SMS и MMS-сообщений, содержащих гиперссылки и изображения. Такие сообщения необходимо незамедлительно удалять, не переходя по ссылкам, указанным в тексте.

Особое внимание стоит уделить ситуации, когда гражданин размещает в интернете объявление о продаже имущества. Под видом покупателя мошенник может попросить номер банковской карты для перевода денежных средств, а затем, получив доступ к мобильному банку, похитить деньги с счета. В подобных случаях категорически запрещено сообщать реквизиты платежных документов, коды подтверждения и иные конфиденциальные сведения.

Приведенные примеры – лишь часть схем, которыми пользуются злоумышленники. Основной их целью является незаконное завладение вашими

организация №

денежными средствами. Будьте внимательны, бдительны и не поддавайтесь на уловки мошенников.